This is an Engineering Note #1

It is a different kind of video from our standard data card format. No structured sections. No standardized vulnerability ratings. Just my engineering read on something I think matters — and that I think the defense community is not talking about clearly enough.

The subject is the Raytheon Coyote Block 3NK. And the subject behind that subject is the single biggest vulnerability in every attacking drone we have covered in this series.

When I started building out the data cards for this channel, one pattern became impossible to ignore. Every drone we reviewed — the Shahed-136, the Lancet-3, the FPV kamikaze, even the more sophisticated platforms — shares the same fundamental weakness. None of them carries electronics certified for EMI, EMC, or EMP hardening. Not one. Commercial flight controllers. Commercial motor speed controllers. Commercial GPS modules. Commercial processors. All of it assembled into weapons systems with no electromagnetic hardening whatsoever.

That is the Achilles heel. Not the GPS link. Not the radio frequency control link. The electronics themselves.

Now, some people will point to the fiber-optic control link as the solution to this vulnerability. And they are right that fiber-optic links completely defeat radio-frequency jamming. You cannot jam an optical cable. That part of the problem has been addressed. But here is what fiber-optic does not fix. It does not harden the flight controller sitting inside that drone. It does not harden the electronic speed controllers driving the motors. It does not harden the processor's interpretation of the navigation solution. The fiber-optic cable protects the communication channel. It does nothing for the electronics at the end of that cable.

That distinction is the engineering insight that the defense community needs to understand clearly. When a high-power microwave weapon fires, it does not attack the communication link. It attacks the electronics directly. Every wire inside that drone — every cable run from a motor back to the control board, every trace on a printed circuit board, every antenna connection — acts as a receiving antenna for the induced microwave energy. The result is unwanted voltage spikes coupled directly into the control circuitry. The boards short out. The drone falls out of the sky. It does not matter whether

the control link is radio frequency or fiber-optic. The kill mechanism bypasses the control link entirely.

This is not a theoretical vulnerability. This is basic electromagnetic physics applied to unhardened commercial electronics.

Now here is my frustration. I have been watching the defense industry's response to the drone swarm threat, and for the longest time almost nobody was looking at high-power microwave weapons as the answer. The conversation has been dominated by radio frequency jamming, GPS spoofing, kinetic interceptors, and lasers. All of which have merit. But none of which exploit the fundamental Achilles heel the way high-power microwave does.

Raytheon has been the exception. The Coyote Block 3NK is, as far as I can tell, the only fielded weapon system that has looked at this problem correctly and built the right solution around it. They took a small autonomous drone, put a miniaturized high-power microwave payload on it, and flew it close enough to the target that you do not need an enormous ground-based emitter to generate the required field strength. Proximity solves the power problem. One Block 3NK can fly into a swarm of attacking drones and repeatedly fire its high-power microwave. The swarm's electronics are not hardened. They short out. The drones fall. And the Block 3NK recovers and flies again.

Reusability is the other piece of this that I want to emphasize. One Block 3NK can engage multiple drones per sortie. And if you need to kill a swarm of 100 drones, you might put up 4 Coyote drones, as they can communicate with each other to optimize their attack on the swarm.

That directly addresses what military planners call the magazine depth problem — the situation where you run out of interceptors before you run out of incoming threats. A kinetic interceptor fires once, and it is gone. The Block 3NK fires, recovers, refurbishes, and fires again. The cost per engagement decreases with each reuse. When you ask how much it costs to shoot down a drone with a high-power microwave weapon, the answer approaches the cost of the electricity used to generate the pulse, divided across every engagement that platform makes in its operational life.

I have seen figures suggesting costs approaching eighty-seven cents per engagement for directed energy systems at scale. Lasers show similar economics. Compare that to a Patriot interceptor at four million dollars per shot, or an S M-6 at four point three million, fired at a drone worth fifty

thousand dollars. The math of the current intercept approach is simply not sustainable at the scale of threat the convergence thesis predicts.

The range limitation of directed energy systems is real — I want to be honest about that. A ground-based high-power microwave system or laser has to project sufficient energy over a distance to achieve the field strength needed at the target. That is a physics problem that does not disappear. But Raytheon's drone-based approach sidesteps that limitation by bringing the emitter to the target. You do not need a massive ground installation projecting energy over kilometers. You need a small drone that flies within meters of the threat and fires at point-blank range. The required field strength drops dramatically. The system becomes practical and cost-effective to produce.

My engineering conclusion is this. Between high-power microwave weapons and lasers — with high-power microwave as my primary pick for the swarm problem specifically — I believe the cost-benefit ratio that makes drone swarming a viable offensive strategy begins to collapse. When you can engage an entire swarm with a single reusable platform at a cost approaching cents per engagement, the attacker's economic advantage disappears. The cost-exchange asymmetry that has defined the drone threat since the Shahed-136 first hit Ukrainian infrastructure — that asymmetry inverts.

Raytheon has its eye on the ball. The Block 3NK is the right approach. I will be watching this technology closely as we continue through the data card series, and I will bring you Engineering Notes whenever I see something that deserves more than a standard vulnerability rating.

The electronics are not hardened. That is the target. Keep your eye on it. On another note, if the attackers do harden their electronics, well, then we must consider a kinetic method to deal with the swarm. We are not there yet, but it is good that we have some other engineering solutions to the swarm challenge.